

Health and Human Services

339.7001

or designee, prior to funding performance beyond the currently funded contract performance period. The Contracting Officer shall ensure that the report and all related approvals are made a part of the official contract/order file. The Section 508 Official or designee shall monitor the Annual Reports, direct corrective measures to improve their submission and quality, and report improvement actions taken to the HHS Office on Disability.

339.203 Approval of exceptions.

(a) Procedures to document exception and determination requests are set forth in the OPDIV/STAFFDIV Section 508 Implementation Plans required by paragraph 4.1 of the HHS Section 508 policy.

(b) In the development of an AP or other acquisition request document, the Contracting Officer shall ensure that all Section 508 commercial non-availability or undue burden exception determination requests for applicable EIT requirements are: (1) Documented and certified in accordance with the requirements of paragraph 4.3, Section 508 Compliance Exceptions, of the HHS Section 508 policy; (2) signed by the Project Officer; (3) approved by the OPDIV Section 508 Official or designee; and (4) included in the AP or other acquisition request document provided by the Project Officer to the contracting office.

(c) In instances where a technical evaluation has been performed, and no organization's proposed products or services meet some or all of Section 508 accessibility standards, in order to proceed with the acquisition, the Contracting Officer shall provide an exception determination request along with the technical evaluation panel's assessment of the Section 508 evaluation factor to the designated Section 508 Official or designee for review and approval/disapproval. *See 315.304* regarding obtaining approval of technical evaluation panel assessments by the Section 508 Official or designee. The Contracting Officer shall include the Section 508 Official's or designee's approval/disapproval of the exception determination request in the official contract file and reference it, as appropriate, in all source selection docu-

ments. For further information, *see* paragraphs 4.3, Section 508 Compliance Exceptions, and paragraph 11, Appendix A, of HHS Section 508 policy—*see* Section 508 policy on HHS Office on Disability Web site.

Subpart 339.70—Use of General Services Administration Blanket Purchase Agreements for Independent Risk Analysis Services

339.7000 Policy.

GSA has established government-wide BPAs for independent risk analysis services, including verification and validation of in-house risk assessments. For information on ordering procedures, *see* the attachment to OMB memorandum (M-08-10), Use of Commercial Independent Risk Analysis Services Blanket Purchase Agreements (BPA), dated February 4, 2008, available on the OMB Web site. HHS policy is for contracting activities to use the GSA BPA sources to the maximum practicable extent.

339.7001 Request for approval to make an award to other than a GSA BPA holder.

The Contracting Officer, in conjunction with the OPDIV/STAFFDIV Chief Information Security Officer (CISO), may determine, as part of conducting market research for independent risk analysis services expected to exceed the micro-purchase threshold, that obtaining the required services from a source other than a GSA BPA holder will result in the best value to the Government. In that event, the Contracting Officer shall prepare a request for approval at least 15 business days prior to the planned date of the contract or order award and forward it through the HCA and the OPDIV/STAFFDIV CISO for concurrence, to the SPE. The SPE shall coordinate the processing of the request with the CAO and the HHS CIO. The request for approval shall briefly describe the services required, indicate the intended source's pricing and other terms and conditions, and provide the rationale for award to the intended source rather

than the GSA BPA holders. The request may include additional supporting rationale to document the best value decision, as appropriate.

339.7002 Notice of intended award.

The CAO, or designee, in conjunction with the HHS CIO, will review the Contracting Officer's request for approval to make an award to other than a GSA BPA holder for independent risk analysis services and either approve or disapprove the request in writing. If the CAO, or designee, approves the request, upon approval, the CAO, or designee, shall send a notice of intended award to the designated GSA BPA Contracting Officer, with a copy to OMB's E-Government and Information Technology Administrator, at least 10 business days prior to the date of the proposed award explaining how it provides the best value to the Government. In the event of unusual and compelling urgency, the CAO, or designee, shall provide the notice of intended award to GSA as soon as practicable.

Subpart 339.71—Information Security Management

339.7100 Definitions.

As used in this subpart, the following definitions shall apply:

Adequate security means, in accordance with OMB Circular A-130, Management of Federal Information Resources, Appendix 3 (Security of Federal Automated Information Resources), security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Federal information means, in accordance with OMB Circular A-130, Management of Federal Information Resources, Appendix 3 (Security of Federal Automated Information Resources), information created, collected, processed, disseminated, or disposed of by or for the Federal Government.

Federal information system means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

Information means, in accordance with OMB Circular A-130, Management of Federal Information Resources, Appendix 3 (Security of Federal Automated Information Resources), any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information infrastructure means the underlying framework that information systems and assets rely on in processing, transmitting, receiving, or storing information electronically.

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide—

(1) *Integrity*, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;

(2) *Confidentiality*, which means preserving authorized restrictions on access and disclosure, including means of protecting personal privacy and proprietary information;

(3) *Availability*, which means ensuring timely and reliable access to and use of information; and

(4) *Privacy*, which means regulating the appropriate collection, maintenance, use, and dissemination of personal information by Federal executive branch agencies. It essentially prohibits disclosure without consent.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services) and related resources.